REMARKS/ARGUMENTS

The Office Action mailed October 31, 2007 has been received and the Examiner's comments carefully reviewed. Claims 1-20 are rejected. Claims 1, 11, 12, 14, 17 and 20 have been amended. For at least the following reasons, Applicants respectfully submit that the pending claims are in condition for allowance.

Claim Rejections

Claims 1-10, are rejected under 35 U.S.C. 103(a) as being unpatentable over Mache (US 2001/0002929 A1) in view of Perrig et al. ("Efficient Authentication and Signing of Multicast Streams over Lossy Channels", 2000) (hereinafter "Perrig"). Claims 11-14, 16-20 rejected under 35 U.S.C. 102(b) as being anticipated by Perrig.

With regard to Claim 1, the Office Action states that "Mache discloses a method for signing transmission from a broadcast server to a client comprises; obtaining a data block that is scheduled for transmission in a next from (para. 0016, lines 1-2; 0037, lines 1-2); selecting a secret key that is associated with the client device for a number of data blocks (para. 0014, lines 3-6; para. 0017, lines 3-5); computing a set of hash keys using the secret key (para. 0031, lines 1-4; para. 0036, lines 1-4); selecting a hash key that is associated with the data block (see abstract); computing an HMAC value for the next frame using the selected hash key (para. 0037, lines 6-7); periodically signing and transmitting a datum containing the hash key of an earlier or initial frame with a digital signature key (para. 0037, lines 1-4). However Mache does not disclose wherein the next frame includes a number of data blocks; generating a count that is associated with time; wherein the selected hash is a set of hash keys using the secret key and the count; and assembling the next frame such that the data block and the HMAC value appear before the hash key in the frame transmission." The Office Action states that "Perrig discloses wherein the next frame includes a number of data blocks (page 2 col. 2, lines 1-7); generating a count that is associated with time (page 7 col. 1, 3rd paragraph); wherein the selected hash is a set of hash keys using the secret key is an intrinsic property of the claimed invention as the prior art discloses a hash chains which include more than one hash keys (page 2 col. 2, lines 1-7); and assembling the next frame such that the data block and the HMAC value appear before the hash key in the frame transmission (page 2 col. 2, lines 1-7; page 3 col. 3, lines 38-43 page 4 col. 2, lines 38-43)." The Applicants respectfully disagree, but have amended the Independent Claims to more clearly define the invention.

As amended, Claim 1 recites in part "obtaining a data block that is scheduled for transmission in a next frame; wherein the next frame includes segment groups; wherein each segment group includes a number (n) of data blocks; wherein each of the data block includes a plurality of packets; ... computing a set of hash keys using the secret key (S_n) and the count; ...computing a keyed-hash message authentication code (HMAC) value for the next frame using the selected hash key (S_i)." In contrast, the cited references do not teach computing the HMAC for an entire frame that includes a plurality of packets or computing the set of hash keys using the count.

While Perrig discloses using a time parameter, the Applicants are unable to locate where this time is used in computing the set of hash keys. Instead, Perrig at paragraph 3 on page 7 recites in part that "Scalability is a major concern for a widely deployed system. If every receiver needs to synchronize its time with the sender, the sender could be a bottleneck. A better solution would use distributed and secure time servers. Initially, the sender synchronizes its time with the time server and computes the maximum synchronization error δ_t (S). The sender would periodically broadcast the interval information, along with its δ_t (S) and the current timestamp, digitally signed to ensure authenticity. The receivers can independently synchronize their time to the synchronization server, and individually compute their maximum synchronization error δ_t. Finally, the receivers add up all the δ_t (S) values to verify the security condition." Perrig, however, does not teach computing a set of hash keys using a count that is based on time and using a secret key. Perrig teaches using a "loose time synchronization" since "the only requirement we have is that the client knows an upper bound δ_t on the maximum synchronization error" (See page 6, first paragraph in Section 2.8). In other words, Perrig is only concerned that the receiver gets a sent packet within some predetermined time period. Additionally, Perrig discloses computing a MAC for every packet. At page 3, under section 2.3, Perrig states "Here is a summary of scheme I: The sender issues a signed commitment to a key which is only known to itself. The sender then uses that key to compute a on a packet P_i, and later discloses the key in packet P_{i+1}, which enables the receiver to verify the commitment and the MAC of packet P_i. If both verifications are successful, packet P_i is authenticated and trusted." In other words, each packet is verified. Claim 1, however recites computing a HMAC for a frame that includes a plurality of packets. Since the cited references do not teach computing the HMAC for an entire frame that includes a plurality of packets or computing the set of hash keys using the count, Claim 1 is proposed to be allowable. Claims depending from Claim 1 are proposed to be allowable as they depend on a valid base claim.

Claim 11, as amended, recites in part "retrieving an Rivest Shamir Adleman (RSA) signed datum from a frame; wherein the frame includes segment groups; wherein each segment group includes data blocks; wherein each of the data blocks include packets; ...computing a hash key using a count and a secret key (S_n) that is known by both the server and the client device, wherein the count corresponds to a time stamp." Claim 11 is proposed to be allowable for at least the reasons presented above. Claims depending from Claim 11 are proposed to be allowable as they depend on a valid base claim.

Claim 17, as amended, recites in part "a scheduler that is arranged to provide data blocks to the server for transmission in a next frame; wherein each of the data block includes a plurality of packets; a counter that is arranged to provide a count in the server; a hashing function in the server that is arranged to compute hash keys for the next frame using the count and a secret key." Claim 17 is proposed to be allowable for at least the reasons presented above. Claims depending from Claim 17 are proposed to be allowable as they depend on a valid base claim.

Claim 20, as amended, recites in part "a broadcast receiver that is arranged to receive a transmitted frame, wherein the transmitted frame includes segment groups; wherein each segment group includes data blocks; wherein each of the data blocks include packets; wherein the transmitted frame includes an HMAC value and a data block, and ends with a hash key S_i; a counter that is arranged to provide a count that has a time dependence; a hashing function that is arranged to compute hash keys for the transmitted frame using the count and a secret key." Claim 20 is proposed to be allowable for at least the reasons presented above.

Conclusion

In view of the foregoing amendments and remarks, all pending claims are believed to be allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the applicant at the telephone number provided below.

Respectfully submitted,

MERCHANT & GOULD P.C.

Timothy P. Sullivan
Registration No. 47,981
Direct Dial: 206.342.6254

MERCHANT & GOULD P.C.
P. O. Box 2903
Minneapolis, Minnesota 55402-0903
206.342.6200

27488
PATENT TRADEMARK OFFICE